УДК 681.3.06

БЫСТРОДЕЙСТВУЮЩИЕ АЛГОРИТМЫ ДЕЛЕНИЯ ПОЛИНОМОВ В АРИФМЕТИКЕ ПО МОДУЛЮ ДВА

Ю.Б. Буркатовская, А.Н. Мальчуков, А.Н. Осокин

Томский политехнический университет
E-mail: jgs@tpu.ru, osikin@ce.cctpu.edu.ru

Предложены быстродействующие алгоритмы деления полиномов в арифметике по модулю два, позволяющие работать с данными в параллельном виде: модификация алгоритма одновременного определения старших и младших разрядов частного, а также разработанный авторами матричный алгоритм деления полиномов. Приведён пример реализации на ПЛИС фирмы Altera кодека двоичного циклического помехоустойчивого кода, использующего матричный алгоритм ускоренного деления полиномов.

Использование помехоустойчивых кодов считается основным средством обеспечения требуемой достоверности передачи данных. В частности, двоичные циклические помехоустойчивые коды используются в системах промышленной автоматизации, радиоинтерфейсах, кодеках видеопоследовательностей, шинах передачи данных процессоров. В связи с увеличением скорости передачи данных требуются быстродействующие помехоустойчивые кодеки, которые смогут работать на частоте шины передачи данных.

Основной операцией при кодировании и декодировании двоичным циклическим помехоустойчивым кодом является операция деления полиномов в арифметике по модулю два, поэтому необходимы быстродействующие алгоритмы деления. Обычно полиномы представляются следующим образом:

$$A(x)=(\sum_{i=0}^{n-1}a_{n-1-i}x^{n-1-i});\ B(x)=(\sum_{j=0}^{m-1}b_{m-1-j}x^{m-1-j}), \quad (1)$$

где a_i, $b_j\in\{0,1\}$; $i=\overline{0,n-1}$; $j=\overline{0,m-1}$; $n\geq m$; n – количество разрядов делимого, m – делителя.

В [1] предложен алгоритм деления полиномов в арифметике по модулю два и доказана теорема для математического обоснования основной идеи алгоритма (одновременное определение старших и младших разрядов частного), формулировка которой представлена ниже.

Теорема 1. Если полиномы вида (1) делятся без остатка, то полиномы, полученные из исходных путем изменения порядка следования коэффициентов на обратный ($A`(x)=x^nA(x^{-1})$; $B`(x)=x^mB(x^{-1})$), также делятся без остатка. Полученное таким образом частное будет иметь обратный порядок следования коэффициентов по сравнению с частным от деления исходных полиномов ($C`(x)=x^rC(x^{-1})$).

В данном алгоритме автором было наложено ограничение: младшие разряды делимого и делителя должны равняться 1. Для устранения ограниче-

ний алгоритма нами было сформулировано и доказано следствие из Теоремы 1 [2].

Следствие из Теоремы 1. Полиномы вида (1) делятся с остатком, если $n-p<m$, где p – количество младших незначащих нулей делимого.

Доказательство (от противного).

Обозначим через p количество младших незначащих нулей полинома A. Тогда,

$$A(x)=(a_{n-1}x^{n-1}+...+a_px^p)=$$
$$=(b_{m-1}x^{m-1}+...+b_0x^0)(C_{n-m}x^{n-m}+...+C_px^p)=$$
$$=B(x)C(x);$$
$$x^p(a_{n-1-p}x^{n-1-p}+...+a_0x^0)=$$
$$=(b_{m-1}x^{m-1}+...+b_0x^0)(C_{n-m}x^{n-m}+...+C_px^p);$$
$$(a_{n-1-p}x^{n-1-p}+...+a_0x^0)=$$
$$=(b_{m-1}x^{m-1}+...+b_0x^0)(C_{n-p-m}x^{n-p-m}+...+C_0x^0),$$

если $m>n-p$, то степень $n-p-m<0$.

Что и требовалось доказать.

Примечание: предполагается, что младший разряд делителя ненулевой, иначе степень делителя вычисляется без младших незначащих нулей.

На основании Теоремы 1 и Следствия из Теоремы 1 разработан «Двусторонний алгоритм ускоренного деления полиномов в арифметике по модулю два», при котором одновременно определяются старшие и младшие разряды частного [2]. В отличие от алгоритма [1], данный алгоритм является универсальным (в нём не накладывается никаких ограничений на делимое и делитель) и всегда обеспечивает корректное вычисление частного.

Пусть n – разрядность делимого, а m – разрядность делителя, тогда разрядность частного равна $r=m-n+1$; A – делимое, B – делитель, C – частное, а D – остаток.

Двусторонний алгоритм ускоренного деления полиномов в арифметике по модулю два.

Начало: даны полиномы вида (1).

Шаг 1: Подсчитываем количество младших незначащих нулей делителя, обозначаем его через p. Запоминаем p последних разрядов делимого и отбрасываем их. Получаем новое делимое $A_1=a_{n-1}...a_p=a^1_{n_1-1}...a^1_0$.

Частное $C_1=C_s...C_0$, где $s=n-m$, $C_i=0$, $i=\overline{0,s}$. Полагаем номер шага $i=1$, $r_i=0$, $l_i=s$.

Шаг 2: Если $A_i\neq 0$, подсчитываем количество старших незначащих нулей L_i и количество младших незначащих нулей R_i в делимом $A_i=a^1_{n_1-1}...a^1_0$. Полагаем $l_i'=l_i-L_i$; $r_i'=r_i+R_i$. Отбрасывая в A_i старшие и младшие незначащие нули, получаем новое делимое A_i разрядности n_i. Иначе идём на шаг 5.

Шаг 3: Если число разрядов $n_i\geq 2(m-p)$, формируем двоичное число (новый делитель):

$$B_i=b_{m-1}...b_p\underbrace{0...0}_{q_i}b_{m-1}...b_p,$$

где q_i – число нулей, которые определяются из условия: $m-p+1+q_i+m-p+1=n_i$ (число нулей таково, чтобы разрядности A_i и B_i совпадали). Получаем двоичное число $A_i+1=A_i\oplus B_i$. Заносим в разряды r_i' и l_i' частного единицы (полагаем $C_{r_i'}=C_{l_i'}=1$, $l_i+1=l_i'-1$; $r_i+1=r_i'+1$; $i=i+1$). Идём на шаг 2. Иначе идём на шаг 4.

Шаг 4: Формируем новое делимое $\widetilde{A}$ следующим образом: приписываем в конец $A_i(r_i+1)$ нулей и p разрядов, запомненных на шаге 1:

$$\widetilde{A}_i=a^i_{n_i-1}...a^i_p\underbrace{0...0}_{r_i+1}a_p...a_0.$$

Делим $\widetilde{A}$ на B обычным способом. Обозначим через Z частное от деления, D – остаток $\widetilde{A}=B\cdot Z+D$.

Частное от деления A на B формируем следующим образом: $\widetilde{C}=C\oplus Z$.

Остаток от деления равен D. Идём на шаг 6.

Шаг 5: Частное от деления A на B равно C. Остаток от деления $D=a_p...a_0$. Если остаток D=0, то полиномы делятся нацело.

Шаг 6: Конец.

Исследовав особенности построения двоичных циклических помехоустойчивых кодов, заметив полезные свойства при построении кода с помощью образующей матрицы в систематической форме, мы разработали «Матричный алгоритм ускоренного деления полиномов в арифметике по модулю два» [3].

Введём обозначения

$$A(x)=A'(x)\oplus\tilde{A}(x);\quad A'(x)=\sum_{i=0}^{n-m}a_{n-1-i}x^{n-1-i},$$
$$\tilde{A}(x)=\sum_{i=n-m+1}^{n-1}a_{n-1-i}x^{n-1-i}\quad\text{и}\quad\tilde{B}(x)=\sum_{j=0}^{m-2}g_jx^j.$$

Определим матрицу Z:

$$Z=\begin{bmatrix}z_0\\z_1\\\vdots\\z_{n-m}\end{bmatrix},$$ где $z_i(x)=R_{B(x)}(x^{n-1-i})$ (остаток от деления x^{n-1-i} на делитель $B(x)$), $i\in(\overline{0,n-m})$.

Матрицу Y определим следующим образом:

$$Y=\begin{bmatrix}y_0\\y_1\\\vdots\\y_{n-m}\end{bmatrix},$$ где $y_i(x)=\frac{x^{n-1-i}}{B(x)}$ (частное от деления x^{n-1-i} на делитель $B(x)$).

Матричный алгоритм ускоренного деления полиномов в арифметике по модулю два.

Начало: Даны полиномы вида (1), где A – делимое, а B – делитель.

Шаг 1: Вычислить матрицу Z для полинома $B(x)$:

$$Z=\begin{bmatrix}z_{0,m-2}&\cdots&z_{0,0}\\z_{1,m-2}&\cdots&z_{1,0}\\&\vdots&\\z_{n-m,m-2}&\cdots&z_{n-m,0}\end{bmatrix}.$$

Шаг 2: вычислить матрицу Y для делимых разрядности n:

$$Y = \begin{bmatrix} y_{0,n-m} & \cdots & y_{0,0} \\ y_{1,n-m} & \cdots & y_{1,0} \\ & \vdots & \\ y_{n-m,n-m} & \cdots & y_{n-m,0} \end{bmatrix}.$$

Шаг 3: Вычислить остаток $A' \cdot Z \oplus \tilde{A}$.

Шаг 4: Вычислить частное $A' \cdot Y$.

Шаг 5: Конец.

Для математического обоснования верности алгоритма сформулируем и докажем ниже представленную теорему [3].

Теорема 2. Если $A' \cdot Z \oplus \tilde{A} = 0$, то $A(x)$ делиться на $B(x)$ без остатка, иначе остатком будет являться результат.

Доказательство.

Рассмотрим разложение x^{n-1-i} на $B(x)$:

$$x^{n-1-i} = B(x) \cdot y_i \oplus z_i(x), \qquad (2)$$

где $i = \overline{0, n-m}$; z_i – i-ая строка матрицы Z.

Выражение (2) подставим в $A'(x)$:

$$A'(x) = \sum_{i=0}^{n-m} a_{n-1-i} \cdot x^{n-1-i} =$$

$$= [\underbrace{\sum_{i=0}^{n-m} a_{n-1-i} \cdot y_i}_{\text{частное}}] \cdot B(x) \oplus \underbrace{\sum_{i=0}^{n-m} a_{n-1-i} \cdot z_i(x)}_{\text{остаток}};$$

$$A(x) = A'(x) \oplus \tilde{A}(x) = [\underbrace{\sum_{i=0}^{n-m} a_{n-1-i} \cdot y_i}_{\text{частное}}] \times$$

$$\times B(x) \oplus \underbrace{[\sum_{i=0}^{n-m} a_{n-1-i} \cdot z_i(x) \oplus \sum_{i=n-m+1}^{n-1} a_{n-1-i} \cdot x^{n-1-i}]}_{\text{остаток}}. \qquad (3)$$

Из (3) видно, что остаток равен

$$\sum_{i=0}^{n-m} a_{n-1-i} \cdot z_i(x) \oplus \sum_{i=n-m+1}^{n-1} a_{n-1-i} \cdot x^{n-1-i},$$

что соответствует

$$A' \cdot Z \oplus \tilde{A} = \sum_{i=0}^{n-m} a_{n-1-i} \cdot z_i \oplus \sum_{i=n-m+1}^{n-1} a_{n-1-i} x^{n-1-i}.$$

Что и требовалось доказать.

Следствие из теоремы:

$$A' \cdot Y = \sum_{i=0}^{n-m} a_{n-1-i} y_i, \; A' \cdot Y = \text{частное}.$$

Для быстрого формирования матриц Z и Y, предложим и докажем следующие выражения:

1. $z_i(x) = z_{i+1}(x) \cdot x \oplus z_{i+1,m-2} \cdot B(x)$, где $z_{i+1,m-2}$ – старший разряд z_{i+1}; $i = \overline{n-m-1, 0}$;
2. $y_i(x) = y_{i+1}(x) \cdot x \oplus z_{i+1,m-2}$, где $i = \overline{n-m-1, 0}$.

Доказательство методом математической индукции:

Базис. $i = n-m$. Тогда $z_{n-m}(x) = R_{B(x)}(x^{m-1}) = \tilde{B}(x)$ и $y_{n-m} = 1$, что очевидно.

Индукция. $0 < j < i$. Тогда

$$x^{j+1} = B(x) \cdot y_{j+1}(x) \oplus z_{j+1}(x);$$

$$x^j = B(x) \cdot y_{j+1}(x) \cdot x \oplus z_{j+1}(x) \cdot x =$$

$$= B(x) \cdot y_{j+1}(x) \cdot x \oplus z_{j+1}(x) \cdot x \oplus v_j \cdot B(x) \oplus v_j \cdot B(x) =$$

$$= B(x)[y_{j+1}(x) \cdot x \oplus v_j] \oplus [z_{j+1}(x) \cdot x \oplus v_j \cdot B(x)].$$

$v_j = 1$ если $z_{j+1,m-2} = 1 \Rightarrow v_j = z_{j+1,m-2}$.

Отсюда следует, что $y_i(x) = y_{j+1}(x) \cdot x \oplus z_{j+1,m-2}$ и $z_i(x) = z_{j+1}(x) \cdot x \oplus z_{j+1,m-2} \cdot B(x)$.

Что и требовалось доказать.

Для определения быстродействия алгоритмов деления полиномов в арифметике по модулю два поставлен компьютерный эксперимент, в котором использовались:

- персональный компьютер: Intel Celeron 1 ГГц, Intel 815EPB chipset, SDRAM 512 Мб, HDD 60 Гб;
- операционная система Microsoft Windows XP SP2;
- разработанный программный экспериментальный комплекс [4].

Эксперимент проводился над 30-разрядными кодовыми словами. Использовался образующий полином вида: $x^6+x^4+x^3+x^2+x^1+1$.

Результаты компьютерного эксперимента сведены в таблицу.

Таблица. *Результаты компьютерного эксперимента*

Количество кодовых слов, тыс.	Время работы алгоритма, с		
	Стандартный	Двусторонний	Матричный
1	0,110	0,110	0,080
5	0,410	0,371	0,220
10	0,791	0,761	0,471
15	1,121	1,062	0,651
20	1,422	1,372	0,822
25	1,763	1,752	1,082
30	2,113	2,003	1,222
35	2,413	2,363	1,523
40	2,774	2,704	1,773
45	3,064	2,944	1,923
50	3,425	3,235	2,053

Из таблицы видно, что двусторонний алгоритм в среднем на 4 % быстрее, чем стандартный алгоритм [1], а матричный алгоритм быстрее стандартного в среднем на 40 %.

Преимущество двустороннего алгоритма проявляется при большой длине кодового слова, когда не хватает памяти в системе для размещения матрицы остатков матричного алгоритма. В практических задачах рекомендуется применять быстродействующий матричный алгоритм деления полиномов в арифметике по модулю два.

В качестве примера нами реализован кодек двоичного циклического помехоустойчивого кода с использованием матричного алгоритма деления на ПЛИС фирмы Altera семейства Acex1. Для исполнения на ПЛИС выбрана структура кодека [5], рис. 1.

На рис. 1 обозначены:

- *cw*[*n*-1..0] – входные данные (кодовое слово для декодирования или информационные символы для кодирования);
- *cb*[*r*-1..0] – контрольный блок;
- *S*[*r*-1..0] – синдром ошибки;
- *ib*[*k*-1..0] – информационный блок;
- *codec* – входной сигнал, который переключает кодек в режимы кодирования и декодирования;
- pe_i – позиция *i*-ой ошибки;
- f_{ei} – исправляющая комбинация для *i*-ой ошибки, $i\in(\overline{1,ce})$;
- *cwo*[*n*-1..0] – выходные данные кодека, т.е. кодовое слово, если *codec*=1 и информационный блок с сигналом ошибки, если *codec*=0, где *n* – разрядность кодового слова, *r* – разрядность контрольного блока, *k* – разрядность информационного блока.

Логические блоки:

- КС 1 – формирования контрольных разрядов с использованием быстродействующего матричного алгоритма деления полиномов в арифметике по модулю два;
- ПЗУ 2* – вычисления позиций ошибок;
- КС 2* – формирования исправляющей комбинации.

В качестве двоичного циклического помехоустойчивого кода был выбран код БЧХ (31,21), который используется в стандарте формата радиовызова POCSAG. Образующий полином данного кода равен $g(x)=x^{10}+x^9+x^8+x^6+x^5+x^3+1$.

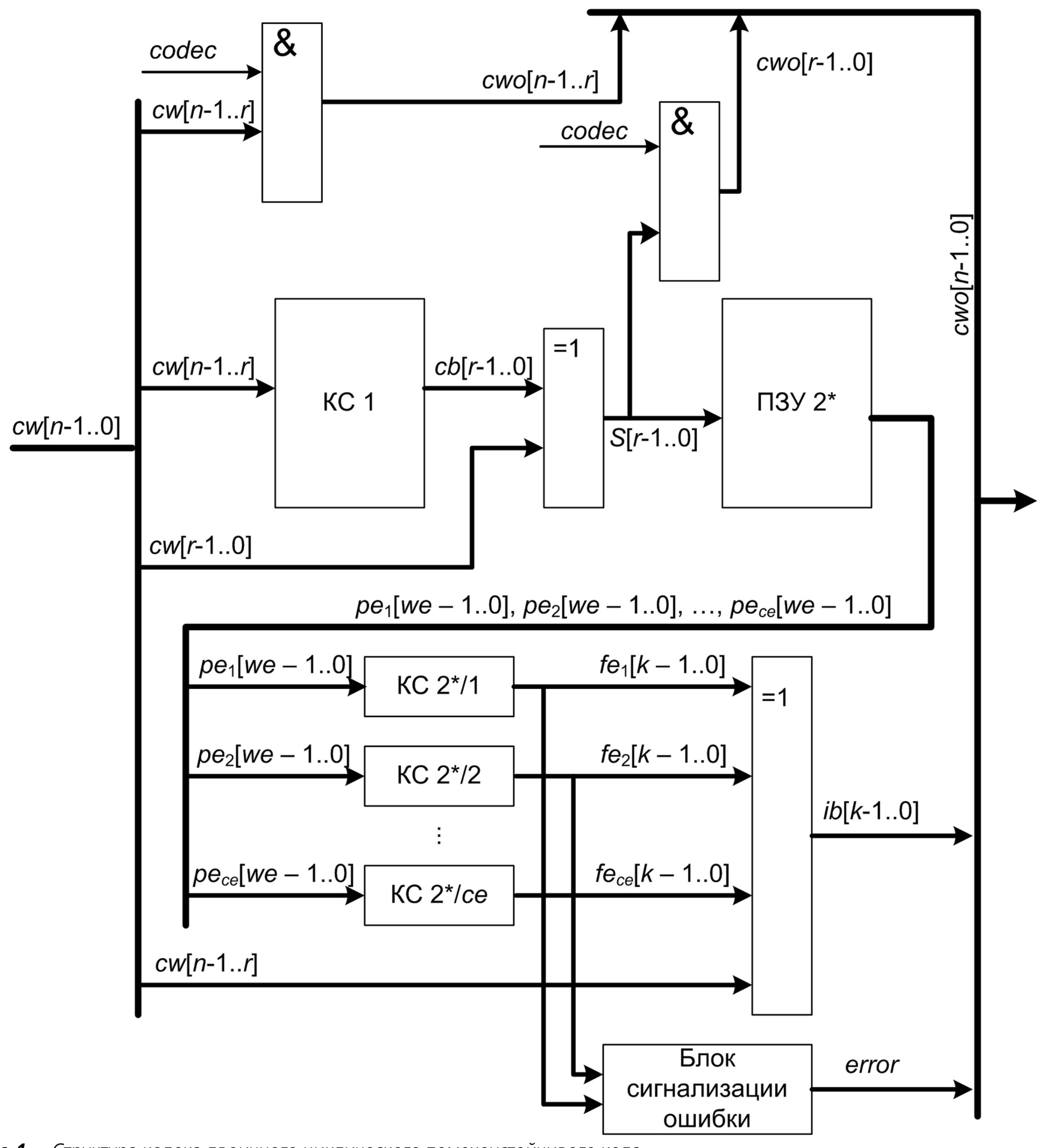


Рис. 1. *Структура кодека двоичного циклического помехоустойчивого кода*

Кодек двоичного циклического помехоустойчивого кода спроектирован с помощью языка описания аппаратуры Verilog. Структура программы кодека представлена на рис. 2.

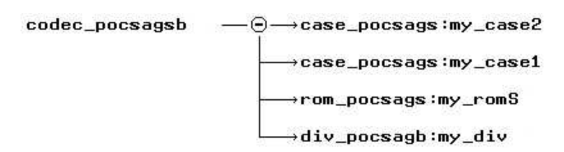


Рис. 2. *Структура программы кодека*

Работа кодека промоделирована в пакете Max+plusII фирмы Altera. Результаты моделирования для ПЛИС EPF10K30ETC144-1 представлены на диаграммах в шестнадцатеричной системе исчисления, рис. 3, 4.

На диаграмме представлены следующие сигналы:

- *data* – входные данные кодека (кодовое слово или информационный блок);
- *fix_data* – исправленное кодовое слово;
- *ready* – сигнал готовности кодека;
- *clock* – синхронизация;
- *div|dividendH* – информационный блок в кодовом слове;
- *div|dividendL* – контрольный блок в кодовом слове;
- *codec* – сигнал, переключающий кодек между режимами кодирования и декодирования;
- *y_div|reminder* – контрольные разряды или синдром ошибки (зависит от сигнала *codec*);
- *_case1|fix_err* – исправляющая комбинация для первой ошибки;
- *_case2|fix_err* – исправляющая комбинация для второй ошибки;
- *error* – сигнал об обнаружении неисправимой ошибки.

Диаграмма моделирования работы кодека в режиме исправления ошибок в кодовом слове представлена на рис. 4. Ошибки находились в двух старших разрядах кодового слова.

В заключение необходимо отметить, что разработанный быстродействующий алгоритм матричного деления полиномов в арифметике по модулю два позволил создать быстродействующий кодек двоичного циклического помехоустойчивого кода. Время работы кодека для ПЛИС EPF10K30ETC144-1 в режимах:

- кодирования 10 нс;
- декодирования 15 нс.

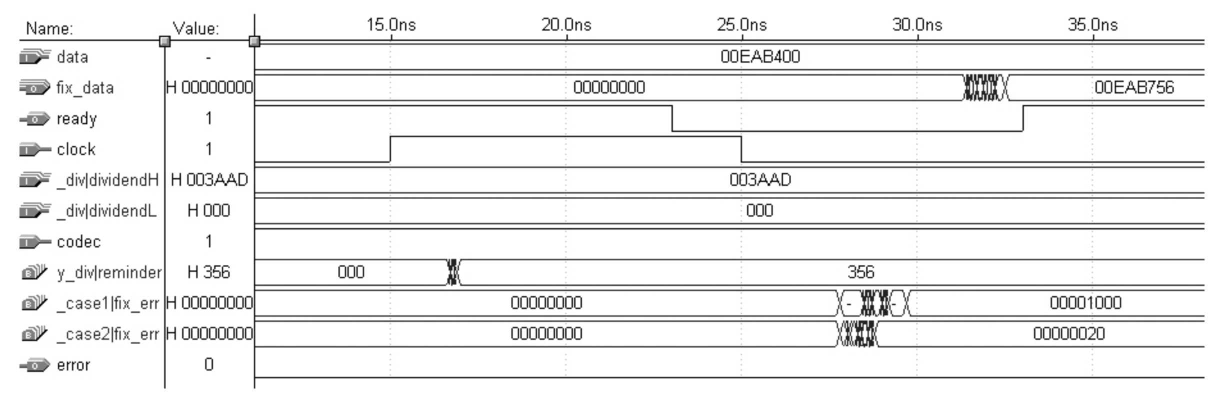


Рис. 3. *Диаграмма моделирования работы кодека в режиме кодирования*

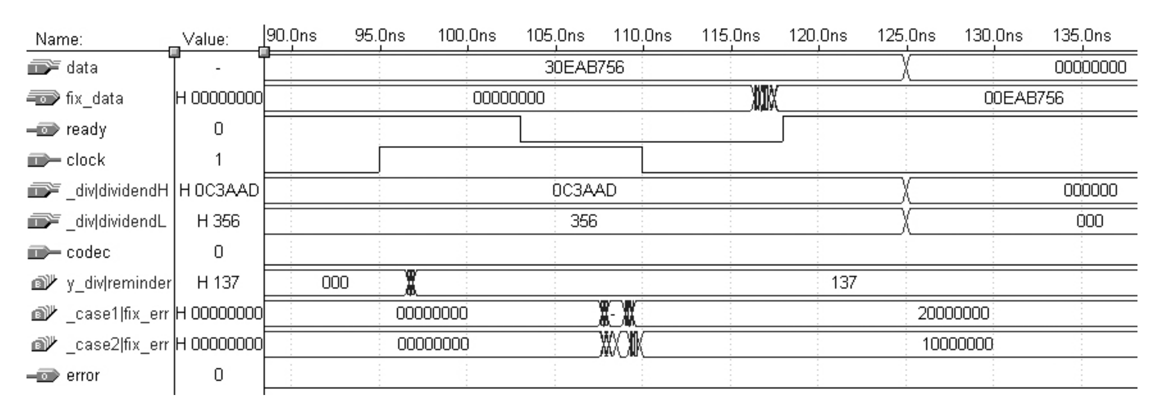


Рис. 4. *Диаграмма моделирования работы кодека в режиме декодирования*

СПИСОК ЛИТЕРАТУРЫ

1. Башин А.Ю. Реализация некоторых алгоритмов для ускорения вычислений на ЭВМ // Автоматика и телемеханика. – 2001. – № 2. – С. 182–189.
2. Bourkatovskaya Y.B., Malchukov A.N., Osokin A.N. Algorithms of accelerated division on modulo 2 // Proc. 7th Korea-Russia Intern. Symp. on Science and Technology "KORUS 2003". – Republic of Korea: University of Ulsan, 2003. – V. 2. – P. 189–193.
3. Буркатовская Ю.Б., Мальчуков А.Н., Осокин А.Н. Алгоритм ускоренного деления полиномов в арифметике по модулю два с использованием матричной арифметики // Современные техника и технологии: Сб. трудов X юбилейной Междунар. научно-практ. конф. студентов, аспирантов и молодых учёных. – Томск, 2004. – Т. 2. – С. 171–173.
4. Мальчуков А.Н. Программная реализация алгоритмов деления полиномов в арифметике по модулю два // Молодежь и современные информационные технологии: Сб. трудов регион. научно-практ. конф. – Томск, 2004. – С. 32–33.
5. Буркатовская Ю.Б., Мальчуков А.Н., Осокин А.Н. Реализация кодека помехоустойчивого двоичного циклического кода в потоке параллельных данных на ПЛИС // Средства и системы автоматизации: Матер. V юбилейной Всерос. научно-практ. конф. – Томск: Изд-во ТУСУР, 2004. – С. 102–105.

УДК 553.411.071.242.4+550.4